Protecting Wastewater Infrastructure Assets...

ASSET BASED VULNERABILITY CHECKLIST FOR WASTEWATER UTILITIES

amsa

AN AMSA CHECKLIST

Protecting Wastewater Infrastructure Assets…

Asset Based Vulnerability Checklist for Wastewater Utilities©

amsa

- ☐ Policies on background checks for potential employees before hiring
- ☐ Policies on periodic criminal checks for existing employees
- ☐ Procedures for employees who may be called to active duty in the military
- ☐ Legal rights afforded to employees who are reservists and members of the National Guard that are called for active military duty
- ☐ Policy to address compensation and benefits for employees who are called to active duty
- ☐ Policy to address compensation and benefits for employees who remain on the job for additional periods during an incident
- ☐ Plan for management to react effectively when some employees may refuse to come to work during an incident
- ☐ Plan to transport personnel to and from work if roads and streets are closed due to police order or physically blocked as a result of an incident
- ☐ Plan to mitigate the concern employees may have for their families' wellbeing during a disaster
- ☐ Management discussion of security issues, emergency response plan, and disaster plan with union representatives

- ☐ Employee photo-identification badges
- ☐ Employee communications equipment to rapidly report incidents
- ☐ Employee monitors for radiation, chemical or biological detection
- ☐ Periodic changes in employee keys and pass-codes
- ☐ Biometric devices to control access to sensitive areas
- ☐ Contractors, vendors and visitors
- ☐ Personal protection devices and first-aid materials at worksites
- ☐ Provisions for food, water and rest for employees that remain on the job for extended periods of time
- ☐ Up-to-date list of all employees, their phone numbers and emergency contact information
- ☐ An employee assistance program to counsel employees and their families on life-crisis management
- ☐ Weapons at utility facilities

- ☐ Employee training to properly handle a threat that is received in person, by phone, by e-mail, by U.S. mail or by other delivery service
- ☐ Employees know the procedures to follow should an incident occur
- ☐ Management knows whom to contact to report a threat or emergency
- ☐ Procedures for determining when and how to evacuate a building
- ☐ Employee training in security measures
- ☐ Employee training in emergency preparedness in accordance with the utility's adopted plan
- ☐ Employee training to detect symptoms of a chemical or biological attack
- ☐ First aid training for employees

- ☐ Emergency response and disaster recovery plans updated and distributed
- ☐ Plan testing for workability
- ☐ Management contact with law enforcement agencies, fire departments, Hazardous Materials (HazMat) teams, and the local office of the Federal Bureau of Investigation (FBI). Coordination of emergency response and disaster recovery plans with these agencies

- ☐ "As-built" drawings up-to-date and easily accessible for use during an incident
- ☐ A comprehensive contact list for employees that includes names and phone numbers of local law enforcement and fire protection agencies, para-medics, emergency response teams, the local FBI office, and the Center for Disease Control
- ☐ Protection from public disclosure of documents and electronic information that reveal vulnerabilities
- ☐ Designated secure location for management to meet and strategize a response to incidents
- ☐ Availability of paper and electronic copies of emergency response information
- ☐ Procurement records

Association of Metropolitan Sewerage Agencies

1816 Jefferson Place, NW Washington, DC 20036-2505 • 202/833-AMSA

info@amsa-cleanwater.org • *http://www.amsa-cleanwater.org*

ASSET: INFORMATION TECHNOLOGY 21

Policies and Planning 22

- ☐ Policies to govern and monitor Internet access and use
- ☐ Asset Classification and Control Procedures
- ☐ Access Controls and Procedures relating to both Internal and External Users
- ☐ Emergency response plans' guidance on communications options during a total loss of telephone, radio, or Internet communications

Protection 23

- ☐ Screening of network traffic for viruses and attacks; virus protection for computers
- ☐ The utility's network has a security architecture implemented for external communications
- ☐ Access via modem to the utility's wide area network (WAN)
- ☐ Vulnerability/penetration evaluations or tests on utility networks
- ☐ Modems attached to end-user desktop systems on the secure local area network (LAN)
- ☐ Local/backup power supply in the event of loss of electric utility supply

SCADA 24

- ☐ Single points of failure in the supervisory control and data acquisition (SCADA) system
- ☐ Periodic identification and backup of "operational-critical" applications, databases, and to an off-site facility
- ☐ Vulnerability/penetration tests on SCADA systems
- ☐ The SCADA system connection to the LAN/WAN
- ☐ Secure locations for the SCADA system components (RTUs, central monitoring)

ASSET: CUSTOMERS 25

Communications 26

- ☐ Utility customers have information about the planning the utility has done, and procedures it has in place, to mitigate the effect of service interruptions
- ☐ Customers have information to cope with service interruptions
- ☐ Discussions of emergency planning efforts and possible consequences that may result with the appropriate regulatory agencies
- ☐ Boilerplate draft press releases and public notices for use during an incident
- ☐ A trained spokesperson as point-of-contact for the media
- ☐ Management meetings with representatives of the jurisdiction's HazMat team, fire/rescue department and law enforcement agency to assure that the utility will be made aware of any hazardous materials that might enter the sewer system during an incident
- ☐ Advising industrial, educational and government customers to examine their internal collection systems for vulnerabilities and share the information with the utility
- ☐ Customers are aware of what activities they should report (and who to call) if they witness something unusual with a utility vehicle, employee, or system asset

Finance 27

- ☐ Access to funds and investment records
- ☐ Coordination with billing agency (in many cases, such as the local water supplier, tax collector, or other local entity) to assure continued collection of wastewater charges and fees during an incident and recovery
- ☐ Maintenance of sufficient reserves to fund operations over a pre-planned period when cash flow may be hampered due to interruption in mail or electronic funds transfer service, delay in revenue submittal from the water supplier, or other adverse event
- ☐ Availability of a contingency line item or reserves to pay for overtime, tanker trucks and other incident-response actions to maintain basic customer services

Protecting Wastewater Infrastructure Assets...

ASSET BASED VULNERABILITY CHECKLIST FOR WASTEWATER UTILITIES

Association of Metropolitan Sewerage Agencies
1816 Jefferson Place, NW Washington, DC 20036-2505 • 202/833-AMSA
info@amsa-cleanwater.org • *http://www.amsa-cleanwater.org*

Table of Contents

COPYRIGHT NOTICE AND DISCLAIMER

This work contains information on the planning and preparation for crisis and extreme events, and the protection of wastewater utility assets. This work necessarily addresses problems of a general nature. Local, state, and federal laws and regulations should be reviewed as they apply to particular situations.

Knowledgeable professionals prepared this work using current information. There is no representation, expressed or implied, that this information is suitable for any particular situation. AMSA has no obligation to update this work or make notification of any changes to any of the statutes, regulations, information or programs discussed in the work. AMSA's publication of this work does not replace employers' duties to warn and properly train and equip their employees and others concerning health and safety risks and necessary precautions.

Neither AMSA nor its contractor, PA Consulting Group, assumes any liability resulting from the use or reliance upon any information, guidance, suggestions, conclusions, or opinions contained in this work.

Foreword

Wastewater utility managers across the United States are being challenged by the need to assess, secure and protect their organization's assets. To meet this need, the Association of Metropolitan Sewerage Agencies (AMSA) has developed the *Asset Based Vulnerability Checklist for Wastewater Utilities*. This publication was specifically designed to help utility managers and their staffs identify and evaluate a wide range of vulnerabilities that could place their assets – physical plant, people, knowledge base, information technology, and customers – in jeopardy. The *Checklist* is meant to stimulate thought and discussion, covering issues related to general security such as computer hacking, vandalism and more severe events like natural disasters and terrorist activity.

In the wake of the tragedies of September 11, 2001, AMSA – with the support of the U.S. Environmental Protection Agency and the National Infrastructure Protection Center – has undertaken several initiatives that strive to guide and support public wastewater utilities in their efforts to prevent, prepare for and respond to potential crisis situations. AMSA's *Asset Based Vulnerability Checklist for Wastewater Utilities* is complemented by a second publication, the *Legal Issues in a Time of Crisis Checklist*. AMSA's *Legal Checklist* addresses many of the legal issues associated with overall crisis management planning, prevention, and response activities. The publication also explores areas such as employee background checks, insurance issues and negligence.

Work is also underway on a *Risk-Based Vulnerability Self-Assessment Software Tool*, the most comprehensive effort to date on creating an easy-to-use tool to aid wastewater utility professionals nationwide as they assess and overcome vulnerabilities associated with their facilities, employees, computer systems and customers. The *Asset Based Vulnerability Checklist* provides the foundation that will be utilized to produce this software and associated training materials. AMSA's *Risk-Based Vulnerability Self-Assessment Software Tool* is slated for release in late spring 2002.

Under the overarching theme, *Protecting Wastewater Infrastructure Assets*, these three important initiatives should prove to be invaluable tools as public agencies assess potential vulnerabilities and implement desired changes to their management and operations.

January 2002

Acknowledgements

Protecting Wastewater Infrastructure Assets… Asset Based Vulnerability Checklist for Wastewater Utilities© was produced and published by the Association of Metropolitan Sewerage Agencies (AMSA) under the direction of its Board of Directors, Wastewater Infrastructure Security Task Force and Executive Director Ken Kirk.

Special thanks are extended to Chair John C. Farnan, General Superintendent of the Water Reclamation District of Greater Chicago, and the members of AMSA's Wastewater Infrastructure Security Task Force (see page 29 for complete listing) for their invaluable advice, detailed comments and dedication to the *Asset Based Vulnerability Checklist for Wastewater Utilities*©. Their continued support and encouragement will ensure the success of the remaining *Protecting Water Infrastructure Assets* initiatives, such as AMSA's Risk Based Vulnerability Assessment Software Tool, which will be released in July 2002.

This document was prepared by PA Consulting Group in collaboration with SCIENTECH, Inc. PA Consulting Group's primary authors include Kenneth I. Rubin, Senior Partner, and Alan B. Ispass, Managing Consultant. SCIENTECH's primary author was Daniel Rees, Vice President.

This project was funded in part through a cooperative agreement between AMSA and the U.S. Environmental Protection Agency.

AMSA is a national trade association representing over 270 of the nation's publicly owned wastewater utilities. AMSA members serve the majority of the sewered population in the United States and collectively treat and reclaim over 18 billion gallons of wastewater every day. AMSA members are environmental practitioners dedicated to protecting and improving the nation's waters and public health.

Today's increasingly complex threats to the nation's water quality present many legislative and regulatory challenges to the wastewater treatment industry. AMSA has long been recognized as a key water quality resource, and the U.S. Environmental Protection Agency, Congress, states and industry frequently look to AMSA for insight on a wide range of clean water issues.

For additional information on AMSA, please call AMSA's National Office at 202/833-AMSA or visit the *Clean Water on the Web* site at http://www.amsa-cleanwater.org.

Executive Summary

Today, all of America faces challenges never before envisioned. The terrorist attacks of September 11, 2001, and subsequent events have shaken our level of comfort. However, they also provide an opportunity for people, companies, governments and organizations of all types, wastewater utilities included, to focus on preparation for unexpected crises. While for years wastewater professionals have understood the need to plan for extreme events, few have had the urgency or resources to fully focus on them.

The Association of Metropolitan Sewerage Agencies (AMSA) has developed this *Asset Based Vulnerability Checklist for Wastewater Utilities*© to help wastewater utilities plan and prepare for extreme events. This *Checklist* will enable wastewater utilities to better understand the extent to which they are prepared for extreme events such as purposeful attacks and natural disasters. Discussed in more detail below, the *Checklist* is one of the first steps in a broader vulnerability assessment and response planning framework that AMSA is working on.

WHAT THE CHECKLIST IS AND ISN'T

AMSA's *Asset Based Vulnerability Checklist for Wastewater Utilities*© is a tool to help utility managers and their staffs identify and evaluate a wide range of vulnerabilities that could place their assets in jeopardy under extreme events such as terrorism or tornados, as well as less severe events such as vandalism or computer hacking. The *Checklist* is meant to stimulate thoughts, ideas, and discussion. It covers issues related to security from both human and natural occurrences, and is a first step in a comprehensive vulnerability assessment and response planning framework.

The *Checklist* addresses matters of a general nature. As such, it does not attempt to cover every issue for every utility. It does not address matters that should otherwise be covered under good design principles and standard codes of practice, such as redundancy and reliability of unit processes, or conformance with life-safety and fire codes. It does not replace the need for independent, utility-specific judgment and decision making.

Complying with all the items in the *Checklist* will not guarantee that your utility will be free from the effects of an extreme event or a minor infraction; nor is it necessary that your utility implement all of the items in the *Checklist* to substantially reduce its vulnerability to disasters and other extreme events. Some items will require discussion and coordination with utility management, legal counsel, local law enforcement, or other government agencies to assure proper resource allocation, design, and implementation of mitigating actions.

A utility may want to begin with a thorough evaluation of its policies and procedures. Before incurring costs for physical improvements, utilities may be able to make significant progress toward closing their vulnerability gaps by strengthening the methods with which they conduct business, both internally and externally. Such attention may reduce the need for costly capital

improvements, or at the very least, make future improvements more effective. The most effective and efficient improvement plan often is built around existing operational procedures. Once these are strengthened, additional actions to deal with extreme events can be added.

Finally, before beginning any vulnerability assessment, with or without the use of this *Checklist*, utility managers would be well advised to collaborate with their legal counsel to assure compliance with the many local, state, and federal laws and regulations that affect a utility's assets, especially its employees and its customers.

THE FRAMEWORK

This *Checklist* constitutes the first step in AMSA's Asset Based Vulnerability Assessment & Response Planning Framework, which adopts a broad, two-dimensional approach to assess vulnerability, prepare for extreme events, respond should they occur, and restore normal business conditions thereafter.

The first dimension of this framework examines utility assets:

Physical Plant,
People,
Knowledge Base,
Information Technology (IT Platform), and
Customers.

The second dimension of the framework recognizes that there is a process over time that begins with the need for early assessment and planning activities, followed by downstream response actions as a result of an extreme event, and eventually, business recovery activities that occur post-event. AMSA's *Checklist* and forthcoming vulnerability assessment software both focus on the upstream assessment phase of preparedness and steer utilities in the direction of planning for recovery and business continuity. These downstream activities will vary considerably from one utility to the next and generally will be customized to local conditions.

The overall approach of AMSA's Vulnerability Assessment and Response Planning Framework is described briefly in the following paragraphs, and depicted graphically in the flowchart that appears at the end of this section.

Asset Categorization and Identification

At this initial stage, utility managers conduct an early inventory of utility assets in each of the five asset categories and assess, appropriate for their circumstances, whether and the extent to which a range of human and natural events may pose possible threats. Appropriate circumstances may include assessing baseline conditions in each of the five asset categories and formulating quick responses to issues raised in the *Checklist*. At this stage, utility managers can begin to form a general sense of their system's vulnerabilities.

Criticality

Each of the identified vulnerabilities are then assessed to determine the potential for adverse consequences should an event occur. Four levels are suggested as one method to categorize this "criticality": low, moderate, high, and very high. These are subjective categories, and the exact definition of these levels will be location- and condition-specific for each utility, and should be defined in that context.

Existing Countermeasures

After criticality is agreed upon, specific existing measures that already mitigate initial vulnerabilities should be identified. If, for example, perimeter penetration is considered a vulnerability, existing countermeasures that reduce vulnerability, such as fencing, closed-circuit TV (CCTV), and/or electronic access control, can affect decisions on next steps.

Vulnerability Rating

Next, utility managers select a vulnerability rating based on the asset in question, appropriate range and probability of threats, and extent to which countermeasures are already in place. Vulnerability ratings are subjective, from very high to low, and should also be defined in the context of local conditions.

Risk Level

Now that the two fundamental aspects of risk – probability (vulnerability) and consequence (criticality) – have been determined, each vulnerability is evaluated using a two-dimensional matrix. The flowchart shows a four-by-four matrix, but if after defining criticality and vulnerability in the context of local conditions, either or both require a different number of rating levels, the dimensions of the matrix should be changed to suit.

Risk Acceptability

Each level of risk should be defined at this stage. In general, red denotes relative unwillingness to accept risk, whereas green denotes relative willingness to accept risk. In any case, definitions should reflect local conditions, since they are used, in effect, to set priorities for risk mitigation.

Identify and Estimate Cost of Risk Mitigation

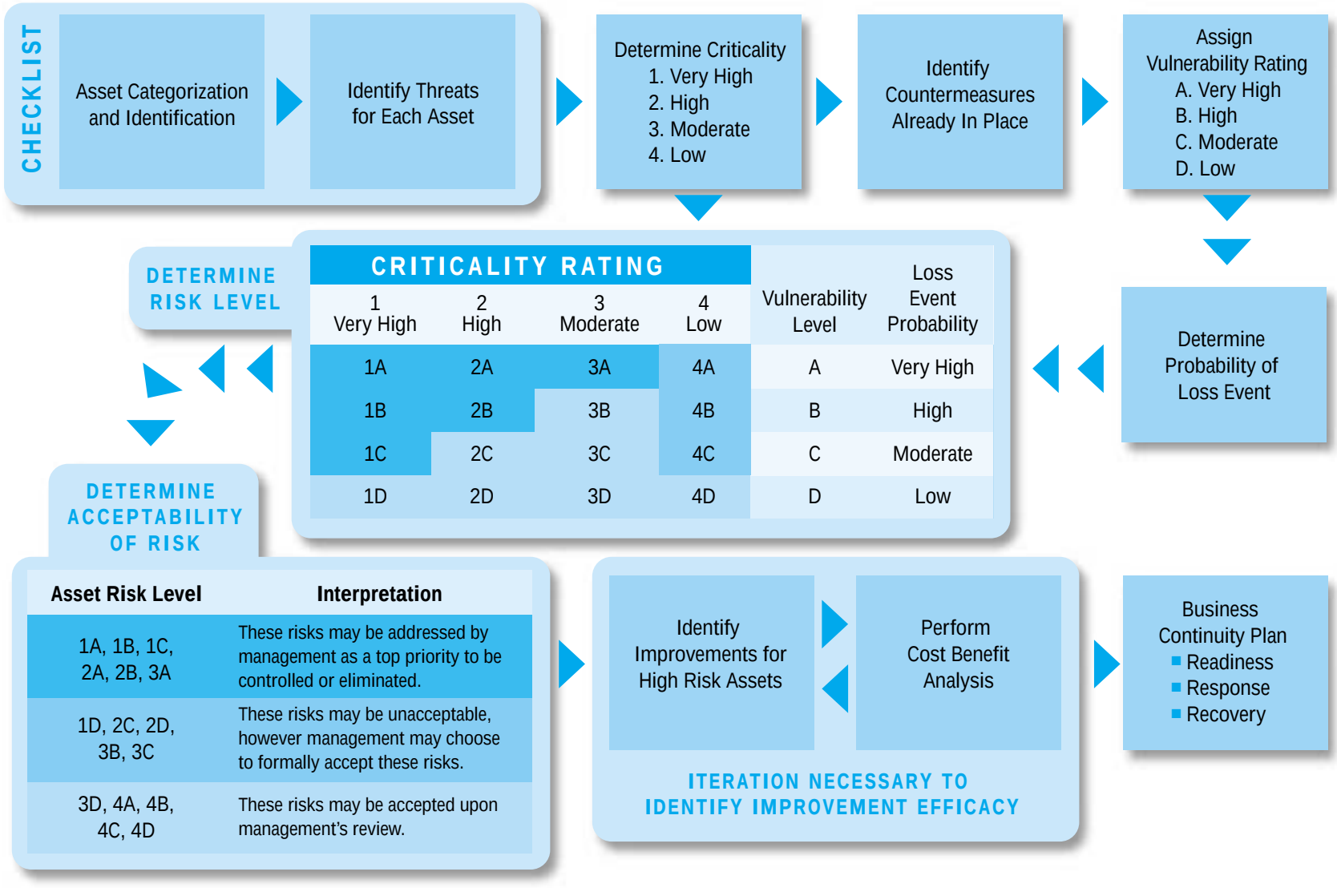
Typically those vulnerabilities with the highest risk receive the highest priority. Utility managers evaluate equipment, technology, structures, procedures, training, communications activities, and the like, that if enacted could mitigate risks, either through reduction of criticality or reduction of vulnerability, or both. Managers may consider seeking these risk-reduction alternatives in an iterative fashion to manage various implementation tools, schedules, and related costs. Costs may play a particularly important role in phasing or scheduling risk mitigation activities, since many of the "hardening" options could require significant investments.

Business Continuity Plan

Business continuity plans map out the "who, what, when, where, and how" for all improvements needed to mitigate or manage known risks. Improvement activities address the questions,

> "What do we need to do to be prepared for human and natural extreme events?" *(Readiness)*
>
> "What do we need to do to respond to human or natural extreme events, should they occur?" *(Response)*
>
> "What do we need to do to restore utility operations to normal after response actions are complete?" *(Recovery)*

Improvement activities will tie back to each of the five utility asset categories, including such actions as capital investments, organizational changes, process reforms, improvements in information management, and enhanced communications. For many utilities, implementation will follow priorities set earlier in this process. Finally, managers may consider an agency-specific schedule for testing business continuity plans, for example, once a year.


CHECKLIST
Asset Categorization and Identification
Identify Threats for Each Asset
Determine Criticality
1. Very High
2. High
3. Moderate
4. Low
Identify Countermeasures Already In Place
Assign Vulnerability Rating
A. Very High
B. High
C. Moderate
D. Low
Determine Probability of Loss Event
DETERMINE RISK LEVEL
CRITICALITY RATING
1 Very High
2 High
3 Moderate
4 Low
Vulnerability Level
Loss Event Probability
1A 2A 3A 4A A Very High
1B 2B 3B 4B B High
1C 2C 3C 4C C Moderate
1D 2D 3D 4D D Low
DETERMINE ACCEPTABILITY OF RISK
Asset Risk Level
Interpretation
1A, 1B, 1C, 2A, 2B, 3A
These risks may be addressed by management as a top priority to be controlled or eliminated.
1D, 2C, 2D, 3B, 3C
These risks may be unacceptable, however management may choose to formally accept these risks.
3D, 4A, 4B, 4C, 4D
These risks may be accepted upon management's review.
Identify Improvements for High Risk Assets
Perform Cost Benefit Analysis
ITERATION NECESSARY TO IDENTIFY IMPROVEMENT EFFICACY
Business Continuity Plan
Readiness
Response
Recovery

I. Asset: Physical Plant

The Checklist

PERIMETER

- ☐ Perimeter physical barriers, such as a fence or wall
- ☐ Locking of perimeter gates
- ☐ Patrolling perimeter by guards or electronic monitoring

ENTRY / ACCESS CONTROL

- ☐ Limiting access to employees or people having valid business at the facility
- ☐ Controlling access by a posted guard or through electronic means
- ☐ Locking of doors and windows
- ☐ Strength of doors, windows and locks
- ☐ Entry codes and locksets
- ☐ Control of visitors, photo identification, sign in and out, and facility escorts
- ☐ Facility tours
- ☐ Security of fill and vent pipes of chemical and fuel storage tanks

SURVEILLANCE

- ☐ Alarming of buildings and critical structures to detect intrusion
- ☐ Alarming of emergency exit doors
- ☐ Monitoring interior of buildings by closed circuit television (CCTV)
- ☐ Site monitoring by CCTV
- ☐ Continuous monitoring of alarms and CCTV with a reporting protocol
- ☐ Connecting alarms and monitoring systems to an uninterruptible power supply
- ☐ Night lighting throughout the facility for surveillance
- ☐ Emergency lighting for evacuation of premises
- ☐ Public address or other warning system to notify people within a facility of an incident
- ☐ Overgrowth of trees and shrubs that may block views of doors and windows

VEHICLE AND MATERIALS DELIVERY MANAGEMENT

- ☐ Parking of private vehicles near buildings and other structures
- ☐ Locking and storage of utility's vehicles
- ☐ Policies for the use and operation of utility's vehicles
- ☐ Monitoring of utility's vehicles via a real-time tracking system
- ☐ Inspection of delivery vehicles
- ☐ Designation of distinct delivery areas for receiving and screening packages prior to their distribution within a facility

COLLECTION SYSTEM

- ☐ Access to sewers in the vicinity of government buildings, financial districts, hospitals and other critical commercial /industrial areas (e.g. chemical manufacturing, defense plants, etc)
- ☐ Secured combined sewer outfalls to prevent entry
- ☐ Security of tributary collection systems operated by other entities
- ☐ Training of pretreatment inspectors and other employees to identify vulnerable points in the sewerage system

HAZARDOUS MATERIAL CONTROL

- ☐ Identification of hazards from process chemicals and other acutely hazardous materials
- ☐ Identification of acutely hazardous materials (AHMs) from adjacent establishments and facilities
- ☐ Tracking mechanism to account for all process chemicals and other acutely hazardous materials received and used at utility facilities
- ☐ Gas detection equipment
- ☐ Information available to employees or others responding to hazardous chemicals or toxins that may be introduced into the sewer system or treatment plant

I. Asset: Physical Plant

OVERVIEW

Protecting a utility's physical assets is key to overall asset protection. Many of the utility's other assets, people, information technology, knowledge base (records, reports, etc.), are housed in utility offices, treatment plants and operations and maintenance shops. Understanding the vulnerability of physical assets, consequently, will provide a clearer picture of the vulnerability of other assets. Likewise, protecting the utility's physical assets often will serve as a first step in protecting many of its other assets.

A utility's physical assets may be a direct target or they may be used indirectly by terrorists or other perpetrators to harm the community. Hazardous chemicals stored at a treatment plant or pump station can be released to adversely affect adjacent areas, for example. Moreover, large diameter sewers may provide hidden access to otherwise protected targets such as government buildings and financial institutions.

The first line of defense is to deny or delay access. This can be accomplished through an analysis of the "layers" of the facility, beginning from the outside. The first layer is the site perimeter. Unobstructed setbacks of at least 100 feet from perimeter barrier to exterior structures can be beneficial but may not be achievable, especially where treatment facilities are located in densely populated urban settings. Thus, analysis of the perimeter barrier and subsequent layers of protection become even more important. The layers following the perimeter are the exteriors of structures (e.g. walls, doors, windows, vents, access hatches), and then the interior spaces with most sensitive areas located high and away from exterior walls and fixtures.

Because physical assets are generally dispersed, an assessment of a physical plant should encompass all infrastructure including office buildings, operations centers, treatment facilities, pump/lift stations, and collection systems, along with their components such as tanks, storage areas, and parking lots.

PERIMETER

Perimeter physical barriers, such as a fence or wall

The most common perimeter barriers include fences, walls, or some combination. Perimeter barriers may not be necessary in all cases if setbacks are sufficient and buffer areas are difficult to cross. For example, the facility could be the surrounded by water, accessible by only one road, or located in a generally difficult to reach location. Fencing materials vary, but are typically chainlink or iron. Walls are typically constructed of reinforced masonry. While most fences and walls act as deterrents and will not stop a determined offender, they can serve to delay an offender by requiring more time to penetrate the barrier and increase the likelihood of their apprehension. Fences and walls can be designed to withstand the impact of certain

vehicles, and constructed of sufficiently strong materials to mitigate the possibility of penetration by cutting or drilling. Climbing can be deterred by making fence and wall height significant (e.g., 8 feet) and topped with barbed wire or similar material, or two parallel fences may be erected with detection devices installed between the fences. Fences or walls should generally still allow viewing of the outside from within and vice versa.

Locking of perimeter gates

Perimeter barriers are most effective if the access through them is secured and controlled. Many facilities will lock gates at all times. Locking mechanisms can be evaluated for their strength to delay, if not deter, intrusion. Automatic gate operators are a possible alternative to manually operated gates because they can reduce the chance that a gate is inadvertently or intentionally left open. For example, such gates could be operated remotely from within a central control station, locally from a guard post, from a vehicle by a transponder, or by a person with a radio-control switch (similar to a garage door opener) or a coded card. However, care must be taken to assure that unauthorized individuals do not enter through an automatic gate immediately behind authorized individuals before the gate fully closes.

Patrolling perimeter by guards or electronic monitoring

Since all perimeter barriers can eventually be breeched, many agencies will find it important to keep the perimeter under surveillance. Some utilities have their own police force while others employ guards as members of the staff. Another alternative is contracting out this service through private companies, or through local law enforcement agencies that allow off-duty police or sheriff deputies to accept outside employment. Training and supervision of guards is an important consideration to ensure they remain alert, reliable and trustworthy. Also possible is the use of electronic surveillance via closed circuit video or motion detection devices, if such devices are monitored by persons who are trained and supervised assuring they are alert, reliable and trustworthy. Some facilities may find that a combination of these alternatives, such as guards and electronic surveillance, is an effective means of perimeter surveillance.

ENTRY / ACCESS CONTROL

Limiting access to employees or people having valid business at the facility

Since citizens and businesses in the community fund the physical assets of a public wastewater utility either directly or indirectly, many utilities have permitted relatively unrestricted access to its buildings and facilities. Not knowing who or why someone is entering a building or facility leaves the utility vulnerable to those wishing to do harm immediately, or plan for offensive action in the future. To the extent allowed by state and local law, utilities may wish to consider limiting access to their facilities to employees or other individuals with a valid need to enter the premises.

Controlling access by a posted guard or through electronic means

This issue is essentially the same as patrolling the perimeter discussed above. Utilities should consider a variety of methods to assure that access is limited to employees and those people having valid business. Recording who comes and goes at all times leaves a record in the event of a breach that could be useful in identifying and locating offenders.

Locking of doors and windows

As with perimeter gates, utilities may evaluate their level of control over indirect access to facility buildings. For example, exterior doors or doors to critical areas may be manually operated once a person's identity is confirmed, or operated through a card key, touch pad, biometric device or remotely from a central station after identity is confirmed.

Strength of doors, windows and locks

Utilities may evaluate whether doors and windows are made of materials that are resistant to easy destruction and properly connected to the structure. For example, some available materials are able to withstand blasts and bullets. Certain films may be applied over windows to strengthen their resistance to breakage. Utilities may evaluate whether locks on doors and windows are resistant to tampering.

Entry codes and locksets

Employee turnover, employee reassignment, loss of keys, purposeful or inadvertent disclosure of entry codes, and surreptitious activity may allow unauthorized entry over a period of time. Therefore, utilities may consider periodically changing entry codes and re-keying locks, and issuing the codes and keys to only those employees still needing access to the secured locations.

Control of visitors, photo identification, sign in and out, and facility escorts

To limit theft from offices, interruption of operations, retaliation by former employees or angry customers and "staking-out" of the utility's premises, utilities may consider new procedures on granting access to their facilities. For example, some utilities may grant access only after a person can substantiate their legitimate business purpose or they are possibly screened against a list of individuals who should not have access. Another option is to escort visitors through the building or facility to protect their safety, limit liability exposure and prevent furtive activities

Facility tours

Providing tours of wastewater treatment facilities is an important part of customer, community and industry relations. Wastewater utilities have a history of encouraging tours to students, teachers, community leaders and visiting dignitaries. While such outreach is important to utilities and the wastewater industry as a whole, a utility may consider evaluating its current procedures for responding to tour requests and conducting facility tours.

Security of fill and vent pipes of chemical and fuel storage tanks

In order to prevent theft and contamination of fuel and chemicals, utilities may evaluate the access to storage tanks and whether barriers and locking devices exist. This may be particularly important at pump stations where perimeter barriers may not be practical, and surveillance may not be feasible.

SURVEILLANCE

Alarming of buildings and critical structures to detect intrusion

Utilities may evaluate whether doors, windows, hatches and other access points on buildings and other critical structures are connected to an alarm system that could alert utility staff or law enforcement authorities to unplanned for access.

Alarming of emergency exit doors

Should an individual gain unauthorized entry into a building, emergency exit door alarms can provide staff knowledge that someone has left without passing through a controlled exit, or force the intruder to find another means of egress whereby they may be delayed and identified.

Monitoring interior of buildings by closed circuit television (CCTV)

Monitoring of building interiors by CCTV is one possible tool to significantly limit criminal activity; however, such monitoring may be considered an invasion of employees' privacy and used by management to observe work habits and performance rather than catch clandestine activities. Should a utility consider using CCTV, it is important to ensure employees are aware of its use through employee policies, including a policy on keeping tapes or disks, and how such information may be used.

Site monitoring by CCTV

Another possibility is augmenting guard patrols on a facility site through the use of CCTV or infrared devices. 24-hour video monitoring of exterior spaces may be thought of as less intrusive by employees, yet still provides a means to detect unauthorized entry. It remains important to ensure that employees are aware of the use of monitoring devices and any utility policy on using this information.

Continuous monitoring of alarms and CCTV with a reporting protocol

Alarms, CCTV and other devices can provide useful information to a utility if intrusion or other furtive activity is detected. Utilities may consider if monitoring 24 hours a day, 7 days a week, 365 days a year is an effective approach. Some utilities may conduct this monitoring via their own staff or through contract services. Utilities can explore a variety of options for staffing the monitoring station and for ensuring that monitoring personnel know the protocol to follow when an alarm is received or video surveillance shows an anomaly.

Connecting alarms and monitoring systems to an uninterruptible power supply

Along with other critical building and facility components, another consideration is whether alarms, CCTV systems and other monitoring devices are connected to an uninterruptible power supply such as an emergency generator with an automatic transfer switch or battery back-up to assure continued operation in a power failure.

Night lighting throughout the facility for surveillance

Utilities can evaluate methods to achieve nighttime illumination within the perimeter of the facility. Should constant lighting adversely affect an adjacent neighborhood, the lighting could be motion activated with manual switching override.

Emergency lighting for evacuation of premises

Utilities can evaluate methods to achieve emergency lighting of interior spaces of buildings and other enclosed structures, including whether backup lighting is available to provide illumination should power be interrupted.

Public address or other warning system to notify people within a facility of an incident

Utilities may evaluate methods to ensure that notification can be made rapidly should a building or entire facility need to be evacuated.

Overgrowth of trees and shrubs that may block views of doors and windows

Utilities may evaluate whether shrubs and trees could prevent surveillance by CCTV and guard patrols.

VEHICLE AND MATERIALS DELIVERY MANAGEMENT

Parking of private vehicles near buildings and other structures

Utilities can evaluate a variety of options to allow sufficient surveillance of people entering buildings and prevent vehicles from being used as weapons. For example, employee and visitor vehicles could be kept at a distance from buildings and other structures. Barriers could be used to prevent parking in locations other than those designated.

Locking and storage of utility's vehicles

Utilities also may evaluate options to prevent theft and damage to utility vehicles, as well as theft of equipment and materials. For example, utility vehicles could be regularly locked and parked in an area within the facility perimeter but within a second barrier "layer" such as a fenced parking lot. Or, employee and visitor vehicles could be prohibited from a secured vehicle area to limit ease of transferring materials from one vehicle to another.

Policies for the use and operation of utility's vehicles

A utility may evaluate its policies for the use and operation of utility vehicles. This could make covert activities more obvious to management, law enforcement and citizens.

Monitoring of utility's vehicles via a real-time tracking system

Some utilities may find that vehicle tracking systems can improve efficiency of service by monitoring the location of employees to more effectively dispatch work crews, better assure proper vehicle use, and help identify early on misuse or unauthorized use of utility vehicles.

Inspection of delivery vehicles

Utilities may consider initiating a procedure to inspect all delivery vehicles prior to the vehicle entering through a facility's gate. Additionally, the utility may require that an assay be performed of any treatment chemicals delivered to a facility before accepting the delivery.

Designation of distinct delivery areas for receiving and screening packages prior to their distribution within a facility

Directing deliveries to a single central location within the facility facilitates monitoring of delivery personnel and their vehicles. Utilities can evaluate policies for staff receipt of and recording of deliveries. For example, a procedure could be established to screen packages to determine if they should be distributed as addressed or held at the delivery area for further scrutiny. An option is to locate a delivery acceptance area outside of the facility's perimeter to allow inspection and assays to be conducted without disruption of operations. Utility personnel can then transfer the package to the facility or accompany the individual making the delivery.

COLLECTION SYSTEM

Access to sewers in the vicinity of government buildings, financial districts, hospitals and other critical commercial/industrial areas (e.g. chemical manufacturing, defense plants, etc.)

To deter the use of the sewer system as a conduit for access to important governmental, institutional and industrial buildings, the wastewater utility could explore methods to secure access to its collection system in these areas. This may involve securing manhole covers to rims with tamper resistant bolts or tack welding, permanent installation of CCTV in the sewers, intrusion detection, or motion detection devices.

Secured combined sewer outfalls to prevent entry

During periods of dry weather large diameter outfall pipes may provide a means to access other portions of the sewer system. One possible approach is to construct barriers at the outfall that do not significantly obstruct flow or trap debris.

Security of tributary collection systems operated by other entities

Many utilities may find it helpful to coordinate with other jurisdictions whose collection systems discharge into its system. Vulnerabilities found in the tributary system(s) can translate into vulnerabilities of the downstream utility's system.

Training of pretreatment inspectors and other employees to identify vulnerable points in the sewerage system

Pretreatment inspectors and other wastewater system employees are at various places in the collection system on a daily basis. They are a helpful source of information on anomalies that may translate into vulnerabilities.

HAZARDOUS MATERIAL CONTROL

Identification of hazards from process chemicals and other acutely hazardous materials

On-site hazardous chemicals can pose public health risks if mismanaged and can become weapons for saboteurs and terrorists. The former is frequently a key element of most utilities' emergency response plans. Utilities may consider enhancing policies and procedures to require extra care in secure storage and safe handling of acutely hazardous materials to minimize risks associated with deliberate releases.

Identification of acutely hazardous materials (AHMs) from adjacent establishments and facilities

Utility plant personnel may become incapacitated or injured due to a release of AHMs from adjacent facilities, whether the release is due to a sabotage, terrorist, or accident condition. Utilities may evaluate their utility emergency response plan to include these off-site hazards, and to assure that plant staff have necessary protection and response equipment and are trained in responding to off-site as well as on-site hazards.

Tracking mechanism to account for all process chemicals and other acutely hazardous materials received and used at utility facilities

Many utilities will find that an accurate inventory on the amount of AHMs will help assure that quantities kept on-site are within limits defined in emergency response plans. Such inventories can signal build-up before on-site accumulation grows to potentially dangerous proportions.

Gas detection equipment

Utilities may consider installing gas detection devices at the plant's headworks or further upstream in the collection system to detect gasoline or other explosive materials that may have been released by accident or to sabotage the system. Consideration may also be given to connect the detection devices to automatic flow gates that will divert the influent flow from the headworks should explosive levels be detected.

Information available to employees or others responding to hazardous chemicals or toxins that may be introduced into the sewer system or treatment plant

Utilities may evaluate their procedures for training employees to react in the event that AHMs are suspected or detected in collection systems and/or treatment works. For example, training may cover personal safety as well as mitigation measures, actions to suspend operations, and flow diversion.

II. Asset: People

The Checklist

HUMAN RESOURCE POLICY

- ☐ Policies on background checks for potential employees before hiring
- ☐ Policies on periodic criminal checks for existing employees
- ☐ Procedures for employees who may be called to active duty in the military
- ☐ Legal rights afforded to employees who are reservists and members of the National Guard that are called for active military duty
- ☐ Policy to address compensation and benefits for employees who are called to active duty
- ☐ Policy to address compensation and benefits for employees who remain on-the-job for elongated periods during an incident
- ☐ Plan for management to effectively react when some employees may refuse to come to work during an incident
- ☐ Plan to transport personnel to and from their place of work if roads and streets are closed due to police order or physically blocked as a result of an incident
- ☐ Plan to mitigate the concern employees may have for their families' well being during a disaster
- ☐ Management discussion of security issues, emergency response plan, and disaster plan with union representatives

PERSONNEL IDENTIFICATION AND PERSONAL WELFARE

- ☐ Employees' photo-identification badges
- ☐ Employee communications equipment to rapidly report incidents
- ☐ Employee monitors for radiation, chemical or biological detection
- ☐ Periodic changes in employee keys and pass-codes
- ☐ Biometric devices to control access to sensitive areas
- ☐ Contractors, vendors and visitors
- ☐ Personal protection devices and first-aid materials at worksites
- ☐ Provisions for food, water and rest for employees that remain on the job for extended periods of time
- ☐ Up-to-date list of all employees, their phone numbers and emergency contact information
- ☐ An employee assistance program to counsel employees and their families on life-crisis management
- ☐ Weapons at utility facilities

PLANNING AND TRAINING

- ☐ Employee training to properly handle a threat that is received in-person, by phone, by e-mail, by U.S. mail or by other delivery service
- ☐ Employees know the procedures to follow should an incident occur
- ☐ Management knows whom to contact to report a threat or emergency
- ☐ Procedures for determining when and how to evacuate a building
- ☐ Employee training in security measures
- ☐ Employee training in emergency preparedness in accordance with the utility's adopted plan
- ☐ Employees training to detect symptoms of a chemical or biological attack
- ☐ First aid training for employees

II. Asset: People

Overview

People are the utility's most strategic asset. Just as employees are the key to the commercial success of the organization, they are also the crucial constituent in assuring suitable analysis of vulnerabilities, proper planning for an emergency, effective reaction to a disaster, and successful recovery from a catastrophe. Most utilities have human resource policies that create a safe workplace, establish lawful and equitable rules, provide for the health and wellbeing of employees, and provide the means for employees to gain knowledge to help their fellow employees, their customers and their community as a whole, especially in times of crisis.

HUMAN RESOURCE POLICY

Policies on background checks for potential employees before hiring

Some utilities may wish to conduct a background check, including proof of citizenship or proper alien status, prior to making an offer of employment to assure that utility management is aware of any criminal convictions, outstanding warrants, or illegal immigration status of a job applicant. Legal guidance should be sought for establishing a policy for such background checks. Some policy elements might include asking all job applicants whether they have been convicted of a felony, or asking for an authorization for background checks. The local law enforcement agency may be able to assist in identifying a method for performing background checks, as not all services and databases are complete.

Policies on periodic criminal checks for existing employees

Some utilities' human resource policies may require employees to notify management should an employee be arrested, convicted of a misdemeanor or felony, or have their visa or work permit expire or revoked. Policies also may allow dismissal of employees under certain conditions related to illegal activities. Subject to legal consultation and appropriate authorization from the employees' bargaining unit, utilities could consider periodic criminal checks of all employees. Again, the local law enforcement agency may be able to assist in identifying a method for performing background checks, as not all services and databases are complete.

Procedures for employees who may be called to active duty in the military

Some utility employees may be members of the National Guard and Armed Forces Reserve Units. Utilities should consider a plan that mitigates the effect of a reduced workforce should these employees be called to active duty.

Legal rights afforded to employees who are reservists and members of the National Guard that are called for active military duty

Legal rights and obligations surround an employee called for active military duty. The Uniformed Services Employment and Reemployment Rights Act of 1994 (USERRA) governs the reemployment, health care, pension and other benefit rights of such employees. In general, the

requirements of the Act: 1) prohibit employment discrimination against employees who take leave for military service and guarantees reemployment when leave is over; 2) provide up to 18 months of continuing health care coverage for employees who are called away for military duty, as well as for their families; and 3) allow employees to make up "missed" contributions to defined contribution plans, and requires employers to make up "missed" matching contributions. Utilities may consider formulating a military leave policy with appropriate legal counsel.

Policy to address compensation and benefits for employees who are called to active duty

While the USERRA sets forth the minimum requirements for employers with regard to employees called to active military duty, some utilities may want to supplement their legally minimum obligations with other policies to reduce the negative financial impacts on their employees and their families during times of crisis. In consultation with legal counsel, utility management may evaluate existing human resource policies to determine compliance with the USERRA and other laws and regulations dealing with employees called to active duty.

Policy to address compensation and benefits for employees who remain on the job for elongated periods during an incident

During a disaster or other emergency situation, employees may be required to stay at a worksite or may be unable to leave due to a government-imposed curfew or the inability to access transportation. Utilities may consider a policy that addresses how employees will be compensated for time spent at the worksite although they may not be actually working, including, for example, whether the cost of meals will be reimbursed by the utility and the extent to which employees would be able to use utility equipment such as telephones and computers for personal needs.

Plan for management to effectively react when some employees may refuse to come to work during an incident

Another possible occurrence involves an understaffing situation resulting from employees calling in "sick" or otherwise refusing to report to work due to their desire to be with their families or the fear of leaving their home. With advice from legal counsel, utilities may consider a policy on this matter that explains the consequences of not reporting to work when required.

Plan to transport personnel to and from their place of work if roads and streets are closed due to police order or physically blocked as a result of an incident

The utility may consider arranging with local law enforcement agencies authorization for employees essential to operations during a disaster or other emergency to pass through roadblocks or to travel to worksites during curfews. For example, these employees could carry official identification, sanctioned by law enforcement, to facilitate their response and work functions. Transportation for employees who may not be able to get to work on their own may be provided by the utility using utility vehicles or hired transport.

Plan to mitigate the concern employees may have for their families' wellbeing during a disaster

Employees can be most effective in their work during an incident if they are assured of their family's wellbeing. As part of emergency planning, the utility may consider urging employees to plan for emergency situations with their families such as arranging meeting places and picking up children from school. The utility also could work with the local emergency planning agency to inform employees and their families of shelter locations that would be available during a disaster or emergency. The utility may want to provide staff to help employees contact their families and relay messages to employees in the field. The utility could also have an Employee Assistance Plan (EAP) to help employees and their families cope with the stresses and emotions that result from an incident.

Management discussion of security issues, emergency response plan, and disaster plan with union representatives

At utilities where employees are represented by bargaining units, management may consider additional measures with union leadership to increase awareness of the planning and policies that will affect their members during a disaster or emergency. One potential issue to be discussed before an incident occurs is compensation during elongated periods on the worksite but not actually working.

PERSONNEL IDENTIFICATION AND PERSONAL WELFARE

Employees' photo-identification badges

At many utilities, employees are issued and required to prominently display photo- identification while at a utility worksite. The photos are generally large and clear, and easily matched to the employee's face. One possible technique to ensure the usefulness of such badges is to have employees who dramatically change their appearance be reissued an updated badge. Another technique is ensuring that individuals who leave the utility return their badges along with other access devices. Periodic changes in badge design and new badge issuance to all employees can help thwart the use of a badge by a former employee who "lost" their badge and could not return it upon leaving the utility.

Employee communications equipment to rapidly report incidents

Utilities may consider a variety of methods to provide employees a means to communicate an imminent emergency or personal distress. For example, while those who work in offices may have telephones available, workers in the field or in various places in a facility may need a different tool to request assistance if needed. For example, these employees could carry a two-way radio connected to a reliable system or a personal distress alarm.

Employee monitors for radiation, chemical or biological detection

Another possible tool to consider is the availability of personal monitors that detect radiation, chemical or biological hazards (as the technology becomes available) for crisis events.

Periodic changes in employee keys and pass-codes

Many utilities may find it helpful to change keys and pass-codes periodically to assure former employees and others do not have access to facilities and secure areas.

Biometric devices to control access to sensitive areas

Another possible technology involves the use of biometric devices as access control to critical areas. Biometric devices measure and analyze unique biological data for recognition of individuals. Biometrics can add verification to the identification that cards, keys and pass-codes provide.

Contractors, vendors and visitors

Utilities may evaluate their policies for admitting non-utility employees to the facility. For example, the policy could require that identification be shown and/or that a valid reason for needing access to utility facilities be provided. Many facilities may choose to allow contractors, vendors, delivery persons or other visitors access to the facility only with an escort. Additionally, utilities may want to consider requiring construction contractors' personnel working within a secure facility to go through the same security procedures as utility employees, or have a barrier installed around the perimeter of the construction activity.

Personal protection devices and first-aid materials at worksites

Many utilities may include in their emergency planning considerations for protecting employees at a facility from exposure to hazardous materials. For example, given that in a disaster or other emergency, response from paramedics and rescue units may be delayed, a utility could keep in stock first-aid materials to tend to significant injuries to several people.

Provisions for food, water and rest for employees that remain on the job for extended periods of time

Utilities may consider setting aside areas at some utility facilities to store bottled water and non-perishable food to be used by employees should an incident occur that requires long-term stays at work and the inability to reach other supplies. These contingent provisions could be purchased annually and, if not used, donated to a local food bank. Additionally, cots and blankets could be stored to make overnight stays at facilities more comfortable for employees.

Up-to-date list of all employees, their phone numbers and emergency contact information

An up-to-date employee contact list is an important asset in any emergency situation for several reasons. Employees may need to be given instructions on reporting for work; in a disaster, it is important to be assured that all employees are accounted for; and, should an employee be injured, a designated relative or friend can be notified without delay.

An employee assistance program to counsel employees and their families on life-crisis management

Disasters and other emergencies can have a devastating effect on employees and their families. Utilities could consider working with an Employee Assistance Program (EAP) that can provide counseling in crisis situations as part of their employees' benefit package to provide a free or low-cost means for employees and their families to receive professional counseling in times of extreme events.

Weapons at utility facilities

Employees may, at times, carry firearms or other weapons on their person, in their vehicles or in their handbags or briefcases. While these employees may have government issued permits, the utility may want to discuss with their legal counsel the possibility of establishing a policy to prohibit firearms and other weapons from being brought on to utility property. The policy may also cover non-employees, as well as hunting on utility-owned property. Additionally, the policy may include the circumstances and procedures that would govern the detection of weapons and action to be taken for policy violation.

PLANNING AND TRAINING

Employee training to properly handle a threat that is received in-person, by phone, by e-mail, by U.S. mail or by other delivery service

Quick action is imperative to avert possible personal injury and physical damage should a threat be credible. Additionally, regardless of the credibility of a threat, a rapid reporting will benefit law enforcement and may hasten the capture of a perpetrator. Utilities could consider seeking guidance for training employees in this area from local law enforcement agencies.

Employees know the procedures to follow should an incident occur

Utilities may choose to review the status of employee training for reaction to pending disasters or emergencies. For example, simple steps could be developed and communicated throughout the organization. Some options include posting, in work areas, the actions to be taken in order to facilitate reporting in stressful situations when employees may not be able to recall the appropriate procedures or providing employees with a wallet card with key emergency information.

Management knows whom to contact to report a threat or emergency

Coordination with law enforcement agencies is important to provide a clear line of communications for reporting threats or emergency situations. Management may consider reviewing reporting procedures with the utility's governing board members to ensure an effective system is in place for reporting events to community officials, citizens and the media.

Procedures for determining when and how to evacuate a building

To mitigate confusion during a crisis, management may consider evaluating and communicating a clear and concise plan for determining under what circumstances a building or facility should be evacuated, what actions should be performed prior to the evacuation, and how employees should report back to the utility after an evacuation.

Employee training in security measures

Many utilities may consider training for all employees to increase awareness of security issues and the measures to be taken to make utility facilities secure. Another option is to offer personal security training to employees.

Employee training in emergency preparedness in accordance with the utility's adopted plan

Most utilities will have an emergency preparedness plan available to all employees. The utility could consider additional training to ensure that all employees understand their individual responsibilities and their role in the organization during a disaster or other emergency situation. One possibility is to hold table-top or mock exercises to assure employees are familiar with procedures and policies that should be followed during an actual incident.

Employees training to detect symptoms of a chemical or biological attack

With the possibility of chemical or biological attacks a reality, utilities may consider employee training on the indications of a chemical or biological attack. Such training might cover physical evidence such as oily substances deposited on surfaces, changes in an individual's health, or upsets in the wastewater treatment process.

First aid training for employees

Utilities may consider first aid courses for employees, possibly at no charge. Trained and possibly first-aid certified persons throughout the utility can help to mitigate the effects of a disaster and save lives. Utilities can contact their local chapter of the Red Cross to pursue the initiation of such courses.

III. Asset: Knowledge Base

The Checklist

PLANNING

- ☐ Emergency response and disaster recovery plans updated and distributed
- ☐ Plan testing for workability
- ☐ Management contact with law enforcement agencies, fire departments, HazMat teams, and the local office of the FBI. Coordination of emergency response and disaster recovery plans with these agencies

CRITICAL BUSINESS DOCUMENTS

- ☐ "As-built" drawings up-to-date and easily accessible for use during an incident
- ☐ A comprehensive contact list for employees that includes names and phone numbers of local law enforcement and fire protection agencies, paramedics, emergency response teams, the local FBI office, and the Center for Disease Control
- ☐ Protection from public disclosure of documents and electronic information that reveal vulnerabilities
- ☐ Designated secure location for management to meet and strategize a response to incidents
- ☐ Availability of paper and electronic copies of emergency response information
- ☐ Procurement records

III. Asset: Knowledge Base

Overview

A utility's knowledge base includes all of its business-critical information, without which continued operations could be in jeopardy, such as: customer records, technical reports, site plans and maps, standard operating policies, operation and maintenance (O&M) manuals, deeds, legal agreements, and contracts.

PLANNING

Emergency response and disaster recovery plans updated and distributed

Emergency response and disaster recovery plans most likely exist in every utility. Often, however, they are not reviewed or updated on a regular basis. Updating these plans periodically, say every two years, enables a utility to incorporate new technologies, additions to staff, additions to physical plant, and new equipment. Once updated, staff that play a key role in either or both plans can be trained in their roles and asked to participate in general staff training in these areas.

Both plans address natural disasters, fire and explosions, hazardous material contamination and purposeful destruction such as terrorism

Many emergency response and disaster recovery plans exclude extreme natural disasters as well as terrorist events because their likelihood is low. Given recent events, however, utilities should consider revisions to these plans to fully explore more possible extreme events.

Plan testing for workability

Many utilities will find it helpful to test emergency response and disaster recovery plans on a periodic basis possibly using table-top or mock exercises to help assure that they are 1) up to date, 2) have all relevant responsibilities clearly identified, 3) address scenarios that reflect current risks. The periodicity of plan testing is up to the utility to decide, commensurate with its assessment of the importance of the exercises and ability of their organization to implement the plans. It will also depend upon the resources available, management confidence in the plans, and specific issues that the utility encounters. In situations where resources are limited, one approach is to perform limited scale testing, i.e., to test only portions of the plan, so that at least some portions of the plan are tested. It is usually not possible to test the plans for all potential incidents. A commonly used practice is to select a different type of incident or scenario each time the plan is tested. The selection of scenarios for testing typically reflects both those incidents that are likely to occur as well as those that may be considered highly improbable.

Management contact with law enforcement agencies, fire departments, HazMat teams, and the local office of the FBI. Coordination of emergency response and disaster recovery plans with these agencies

For criminal, sabotage, and terrorist events, the direct involvement of these organizations from the initiation of the utility response helps to ensure that the best response is implemented in a timely manner. In addition, a continuous dialogue with these organizations helps management identify and assess threats that may not have been considered in utility planning.

CRITICAL BUSINESS DOCUMENTS

"As-built" drawings up-to-date and easily accessible for use during an incident

Especially for older facilities that have had several additions or modifications over the years, it is important that utility staff have up-to-date and accurate sets of drawings of treatment processes and distribution systems to facilitate emergency response actions. It is important that these drawings be easily accessible since response times may be limited.

Duplicates of critical documents (e.g. deeds, leases, MOUs, contracts, local agreements, "as-built" drawings, O&M manuals, customer records, personnel records) kept in a secure off-site location

Procedures to ensure duplicates of critical documents are available in a secure location and also available electronically can help assure continued service to customers in the event of facility evacuation or damage.

A comprehensive contact list for employees that includes names and phone numbers of local law enforcement and fire protection agencies, paramedics, emergency response teams, the local FBI office, and the Center for Disease Control

This information is usually included in emergency response plans but also is helpful when readily accessible to all employees. It supports additional call-outs and accounting for employees following an explosion, fire, or other extreme event. Periodic updating of the contact list also is helpful.

Protection from public disclosure of documents and electronic information that reveal vulnerabilities

Emergency Response Plans, Disaster Recovery Plans, Risk Assessments and similar documents can provide unintentional "road maps" to saboteurs or terrorists. Utilities may wish to explore methods of protecting these documents. Utility legal staff can play a role in ensuring that, where legally appropriate, documents and plans generated are protected from general public disclosure.

Designated secure location for management to meet and strategize a response to incidents

Incidents may render all normal utility office locations unsuitable for meeting and strategizing a response. As a result, it can be helpful to identify a location for management to use if needed during response to major incidents. For example, the location could be protected from any facility hazards, have the necessary information at hand to respond to any facility incident, or have communication capability.

Availability of paper and electronic copies of emergency response information

If electric power, computing facilities, or network access fail, electronic versions of key emergency plans may be unavailable. Thus, it is important that utility management have access to paper copies of emergency response plans, disaster recovery plans, and related documents.

Ordinances, policies and procedures allow lawful mitigation of vulnerabilities and execution of emergency response and disaster recovery actions

In some crises, it may be necessary to suspend operations, divert untreated wastewater, or temporarily exceed discharge limits. Facility management may wish to ensure that ordinances, policies and procedures are in place to enable appropriate, but unusual, management actions where warranted in response to extreme events.

Procurement records

If a crisis occurs that requires relocation of procurement activities, access to vendor lists, purchase orders, and contract documents may be unavailable. Therefore, the utility may wish to consider having duplicate documents available at a secure offsite location, or in an electronic format, to allow purchasing of goods and services to continue from an alternate location.

IV. Asset: Information Technology

The Checklist

POLICIES AND PLANNING

- ☐ Policies to govern and monitor Internet access and use
- ☐ Asset Classification and Control Procedures
- ☐ Access Controls and Procedures relating to both Internal and External Users
- ☐ Emergency response plans' guidance on communications options during a total loss of telephone communications, loss of radio communications, or loss of Internet communications

PROTECTION

- ☐ Screening of network traffic for viruses and attacks; virus protection for computers
- ☐ The utility's network has a security architecture implemented for external communications
- ☐ Access via modem to the utility's wide area network (WAN)
- ☐ Vulnerability/penetration evaluations or tests on utility networks
- ☐ Modems attached to end-user desktop systems on the secure local area network (LAN)
- ☐ Local / back-up power supply in the event of loss of electric utility supply

SCADA

- ☐ Single points of failure in the supervisory control and data acquisition (SCADA) system
- ☐ Periodic identification and back up of "operational-critical" applications, databases, and to an off-site facility
- ☐ Vulnerability/penetration tests on SCADA systems
- ☐ The SCADA system connection to the LAN/WAN
- ☐ Secure locations for the SCADA system components (RTUs, central monitoring)

IV. Asset: Information Technology

Overview

When information technology (IT) vulnerabilities are addressed, robust and flexible technology solutions can be assured to continue to support business functions under a wide variety of conditions. Information technology includes early warning systems, corporate IT security policy, cryptographic system design, contingency planning, IT security awareness, IT security management and organization, security systems testing, and state-of-the-art security technology. Most utilities today have a computer security policy in place that covers not just the corporate network, but also those networks supporting SCADA systems. A subset of this overall policy should be an Internet Access and Use Policy that normally defines the limitations and responsibilities relating to both types of networks respectively.

POLICIES AND PLANNING

Policies to govern and monitor Internet access and use

Use of the Internet from company locations has the potential to introduce vulnerabilities into the utility network by exposing passwords, cookies and other forms of cyber-identification. In consultation with legal counsel, utilities may consider development of policies governing use of the Internet to minimize risks of outside cyber-intrusion. One possible compliance assurance tool is an oversight or monitoring program. Employer disclosure of any monitoring policies to employees is important.

Asset Classification and Control Procedures

The computer security policy/computer security architecture may also include Asset Classification and Control Procedures that include the requirements for maintenance of detailed hardware and software inventories for both the Corporate and SCADA related networks. This information is important not only for reasons of legal compliance with software licensing regulations, but also for contingency planning.

Access Controls and Procedures relating to both Internal and External Users

Potential threats can originate from within the Utility organization as well as from outside the organization. Utilities may consider controlling access to IT secure areas, as well as files and folders on the network. Additionally, regular review of access controls to both internal and external sources may be performed.

Emergency response plan guidance on communications options during a loss of telephone, radio, or Internet communications

Communications via land-lines and/or cell phones, radios, and the Internet may be disabled during an incident. Utilities may consider incorporating alternate communication methods and backup approaches into their emergency response plans.

PROTECTION

Screening of network traffic for viruses and attacks; virus protection for computers

Utilities may evaluate installing a virus protection program to run during start-up or sign-on of every utility computer, and to serve to protect the integrity of data and provide a barrier to data and equipment damage. Another technique is to check individual computers periodically to assure that users have not disabled virus-protection programs (either intentionally or unintentionally) and that the most current software version is installed and operational.

The utility's network has a security architecture implemented for external communications

Most utilities will find it helpful if their IT security architecture includes, but is not limited to, firewalls. This architecture can be designed to provide maximum security while maintaining flexibility. For example, a security framework can include a firewall, an Intrusion Detection System/Network Intrusion Detection (IDS/NID), Access Control List (ACL) in network devices, Authorization and Accounting (AAA), monitoring, policies/procedures, and Virtual Private Networks (VPNs) for secure remote access. Usually, virus protection is also part of this architecture. A common misconception is that a firewall provides all necessary protection; however, without proper processes, firewalls alone create a false sense of security and may compromise overall system security.

Access via modem to the utility's wide area network (WAN)

Direct access to the WAN from an outside connection via modem can provide an easy path for hackers or saboteurs to erase, manipulate or damage utility data and equipment. If it is necessary for the WAN to be accessed via modem, utilities can consider a secure method to authorize users and to limit the activities they can perform remotely. If it is necessary to provide remote access to the WAN via modem, user IDs and passwords can be encrypted. Another option for enhancing security of dial up connections is implementation of a dial back program.

Vulnerability/penetration evaluations or tests on utility networks

In most installations, network configurations change frequently. To help assure the continued robustness of the network against hacking and sabotage, most utilities will find periodic evaluation and penetration tests revealing. "War dialing" (automated calling of all phone lines and numbers into a facility of their Direct Inward Dialing [DID blocks]) is one tool that can be used to detect the presence of modems on assigned telephone lines.

Modems attached to end-user desktop systems on the secure local area network (LAN)

Modems connected to desktop machines create a common vulnerability to computer networks. This can provide an outsider with a conduit into the utility network that circumvents any installed firewall or other protection schemes. For this reason, many utilities do not allow their desktop computers to have modems installed or, at a minimum, have software installed that disables the Local Area Network connection when the modem is in use. These modem connections are also detected using "war dialing" as described above.

Local / backup power supply in the event of loss of electric utility supply

Utilities may investigate back-up power to allow controlled shutdown of processes and SCADA systems as well as backup of critical data.

SCADA

Single points of failure in the supervisory control and data acquisition (SCADA) system

Physical and electronic single points of failure can easily lead to the complete disabling of a SCADA system. Utilities may consider "hardening" the system against potential intruders. Hardening is the activity of making the system less susceptible to tampering and sabotage by assuring the integrity of the communication links, upgrading system components to be able to withstand electromagnetic interference, and incorporating diversity and redundancy so that a single failure will not disable the system.

Periodic identification and backup of "operational-critical" applications and databases to an off-site facility

Intrusion into the SCADA system may damage the operating system, application software, data records, and/or set-point information. Utilities may consider maintaining a complete set of software and backed-up data so that the system can be re-loaded and returned to operation following a serious incident.

Vulnerability/penetration tests on SCADA systems

Security of the SCADA or process control systems are dependent upon several variables including the type of communications used to link Remote Terminal Units (RTUs) to the central terminal unit (e.g. dedicated line, dial-up, fiber, radio frequency, web based, WAN, etc.), access to RTUs and central station, system power supply, and other physical attributes of local IT systems. With regard to the communications aspect, the most direct approach to uncover vulnerability is "penetration testing," either on-site, off-site or a combination of the two, as well as analysis of the current design. Penetration testing can detect vulnerability and security breaches that could be used to attack and penetrate an internal network including databases, process control, confidential documents finance information, email, and other electronically stored information.

The SCADA system connection to the LAN/WAN

Connection of the SCADA system to the LAN/WAN can result in an additional vulnerability to the SCADA system from the Internet or internal saboteur. Utility managers can explore whether LAN/WAN connections to the SCADA have the same level of security and protection discussed above.

Secure locations for the SCADA system components (RTUs, central monitoring)

Utilities may wish to locate SCADA components in a secure building with access limited to authorized utility staff. Another possibility is ensuring electrical connections, to the extent possible, be inside conduit or buried to minimize exposure to sabotage events. Since some incidents may temporarily or permanently impair the monitoring of the process, additional monitoring locations may be considered so that plant operations can continue.

V. Asset: Customers

The Checklist

COMMUNICATIONS

- ☐ Utility customers have information about the planning the utility has done, and procedures it has in place, to mitigate the effect of service interruptions
- ☐ Customers have information to cope with service interruptions
- ☐ Discussions of emergency planning efforts and possible consequences that may result with the appropriate regulatory agencies
- ☐ Boilerplate draft press releases and public notices for use during an incident
- ☐ A trained spokesperson as point-of-contact for the media
- ☐ Management meetings with representatives of the jurisdiction's HazMat team, fire/rescue department and law enforcement agency to assure that the utility will be made aware of any hazardous materials that might enter the sewer system during an incident
- ☐ Advising industrial, educational and government customers to examine their internal collection systems for vulnerabilities and share the information with the utility
- ☐ Customers are aware of what activities they should report (and who to call) if they witness something unusual with a utility vehicle, employee, or system asset

FINANCE

- ☐ Access to funds and investment records
- ☐ Coordination with billing agency (in many cases, such as the local water supplier, tax collector, or other local entity) to assure continued collection of wastewater charges and fees during an incident and recovery
- ☐ Maintenance of sufficient reserves to fund operations over a pre-planned period when cash flow may be hampered due to interruption in mail or electronic funds transfer service, delay in revenue submittal from the water supplier, or other adverse event
- ☐ A contingency line item or reserves are available to pay for overtime, tanker trucks and other incident-response actions to maintain basic customer services

V. Asset: Customers

Overview

Customers are the lifeblood of the utility and the purpose of the utility's existence. As with day-to-day operations, the utility should strive to meet, and if possible, exceed customer expectations when it comes to evaluating vulnerabilities, planning for emergencies and responding to, and recovering from disasters. Communications, service continuation, and financial integrity are the focus of assuring that this very important asset is protected from the effects of a disaster.

COMMUNICATIONS

Utility customers have information about the planning the utility has done, and procedures it has in place, to mitigate the effect of service interruptions

Instilling customer confidence in the utility is critical to meeting customer expectations and achieving customer satisfaction. Utilities can explore effective ways to inform customers about their emergency preparedness and recovery planning activities as one indication of the utility's readiness and preparation to continue service even under a wide variety of extreme events. For example, notes on bills, newsletters, public service announcements and press releases are several vehicles the utility can use to keep customers aware of the utility's concern for continuous, high-quality service.

Customers have information to cope with service interruptions

While customer communications generally may emphasize that the utility has comprehensively planned for emergencies and has contingency plans in place to maintain wastewater services, they may also indicate that there is a remote possibility that wastewater service could be interrupted in a disaster situation. Information can be provided on how customers can cope with the loss of wastewater service and how to mitigate the possibility of sewer backups.

Discussions of emergency planning efforts and possible consequences that may result with the appropriate regulatory agencies

While wastewater utilities are undoubtedly dedicated to maintaining compliance with permit requirements and environmental regulations, a disaster or other emergency may result in an inadvertent sewage overflow or inadequate treatment prior to discharge. With legal counsel's guidance, utility management may consider discussing such possibilities with their state regulatory agency and regional EPA staff, and sharing with them the steps that the utility has taken to evaluate vulnerabilities, plan for emergencies and react to incidences with the goal of maintaining full compliance with permit conditions and regulations. Plans for communicating with the regulatory agencies during an incident can also be established up-front.

Boilerplate draft press releases and public notices for use during an incident

Utilities may wish to evaluate the effects a disaster may have on the wastewater system including interruption of service to customers and adverse environmental impacts. Boilerplate press releases could be drafted for situations that may occur and kept available for adaptation to specific circumstances when necessary. This could save time and effort that would otherwise be necessary to prepare a press release from "scratch" during an incident.

A trained spokesperson as point-of-contact for the media

If the utility does not already have a media spokesperson or public information officer, the utility may consider appointing and training a senior staff member in media relations. Another possibility is to designate an area for reporters, fostering cooperation with the media. It is important for the utility to carefully evaluate information provided to the media for accuracy and current information. Emphasis can be placed on the positive steps that the utility is taking to mitigate the effects of the incident and continue to provide or to restore service.

Management meetings with representatives of the jurisdiction's HazMat team, fire/rescue department and law enforcement agency to assure that the utility will be made aware of any hazardous materials that might enter the sewer system during an incident

As wastewater professionals already know, the majority of people are not aware of how wastewater services are provided or the processes involved in wastewater treatment. Consequently, it is important to discuss with emergency response agencies the effects that hazardous materials entering the sewer system can have on the wastewater infrastructure and on the environment, and how communications can be established if such discharge is possible during an incident.

Advising industrial, educational and government customers to examine their internal collection systems for vulnerabilities and share the information with the utility

Small, private collection systems can harbor the same vulnerabilities as the collection systems of a major public utility. Therefore, to assure the integrity of the utility's wastewater system, it is imperative that tributary collection systems that are not maintained by the utility be evaluated for vulnerabilities and protected against extreme events. Utility managers can facilitate this process by meeting with owners and operators of these collection systems to coordinate planning efforts.

Customers are aware of what activities they should report (and who to call) if they witness something unusual with a utility vehicle, employee, or system asset

Customers can be an excellent source of information for the utility to learn about vulnerabilities and threats to its wastewater system. Customers can add thousands of eyes and ears to surveillance of the utility system, reporting apparent surreptitious activities that may adversely affect the wastewater system. Information can be provided to customers via billing notices or newsletters on what behaviors and actions can be reported and how to report them.

FINANCE

Access to funds and investment records

Utility management may wish to coordinate with its banking institutions and investment managers to assure access to funds and account information is available in crisis situations, and that options exist for withdrawing and depositing funds, as well as continuing the management of investments should normal channels of information and financial transfers be disrupted.

Coordination with billing agency (such as the local water supplier, tax collector, or other local entity) to assure continued collection of wastewater charges and fees during an incident and recovery

Since the vast majority of wastewater utilities are dependent upon the local water supplier to collect its rates and fees from customers, it is important that the wastewater utility reach agreement with its billing/collecting counterpart to assure that revenues will continue to flow into the wastewater utility during a crisis. Discussions with the water utility can include contingency planning for the inability of reading meters and the disruption of mail service or electronic banking transactions. The utility may also consider developing contingent procedures to generate and distribute its own bills and undertake collection activities should its billing/collecting counterpart be unable to do so.

Maintenance of sufficient reserves to fund operations over a pre-planned period when cash flow may be hampered due to interruption in mail or electronic funds transfer service, delay in revenue submittal from the water supplier, or other adverse event

To assure the utility can continue to meet payroll, pay its bills, contract for necessary materials and services, and fulfill its other obligations during a crisis, a non-restricted reserve account can be established to contain sufficient funds to offset delays in collection of regular fees from customers.

A contingency line item or reserves are available to pay for overtime, tanker trucks and other incident-response actions to maintain basic customer services

Even if revenues are unaffected by a crisis, expenses to react and recover from a disaster can be expected to greatly exceed normal operating costs. Therefore, utilities can explore whether sufficient funds are available in a contingency operating line item, or as cash or a short-term investment in a reserve account, to provide for expenses incurred during and immediately after an incident.

AMSA Wastewater Infrastructure Security Task Force

Chair
John C. Farnan
General Superintendent
Metropolitan Water Reclamation District of Greater Chicago
Chicago, IL

James T. Canaday
Engineer-Director
Alexandria Sanitation Authority
Alexandria, VA

Ra'Nell Davis-Hale
Utility Engineer III
Anne Arundel County DPW
Bureau of Utility Operations
Annapolis, MD

John Greeley
Division Manager, Source Control & Lab Services
Clean Water Services
Hillsboro, OR

Gurnie C. Gunter
Director
Kansas City, MO Water Department
Kansas City, MO

Philip Heckler
Deputy Director, Environmental Affairs
New York City Department of Environmental Protection
Corona, NY

Robert W. Hite
District Manager
Metro Wastewater Reclamation District
Denver, CO

Patrick T. Karney
Sewer Director
Metropolitan Sewer District of Greater Cincinnati
Cincinnati, OH

Kumar Kishinchand
Water Commissioner
Philadelphia Water Department
Philadelphia, PA

Michael D. Luers
General Manager
Snyderville Basin Water Reclamation District
Park City, UT

Victor Nolan
Risk and Benefits Manager
Clean Water Services
Hillsboro, OR

H.J. "Bud" Schardein
Community Relations & Emergency Response Director
Louisville & Jefferson County Metropolitan Sewer District
Louisville, KY

Donnie R. Wheeler
General Manager
Hampton Roads Sanitation District
Virginia Beach, VA

AMSA Officers and Board of Directors

PRESIDENT
Gurnie C. Gunter
Director
Kansas City Water Services Department
Kansas City, MO

VICE PRESIDENT
Paul Pinault
Executive Director
Narragansett Bay Commission
Providence, RI

TREASURER
Thomas R. Morgan
General Manager
Montgomery Water Works & Sanitary Sewer Board
Montgomery, AL

SECRETARY
William B. Schatz
General Counsel
Northeast Ohio Regional Sewer District
Cleveland, OH

REGION I
Marian Orfeo
Director of Planning & Coordination
Massachusetts Water Resources Authority
Boston, MA

Paul Pinault
Executive Director
Narragansett Bay Commission
Providence, RI

REGION II
Robert J. Davenport
Executive Director
Passaic Valley Sewerage Commissioners
Newark, NJ

Richard P. Tokarski
Executive Director
Rahway Valley Sewerage Authority
Rahway, NJ

Joel A. Miele, Sr.
Commissioner
NYC Department of Environmental Protection
Corona, NY

REGION III
Kumar Kishinchand
Water Commissioner
Philadelphia Water Department
Philadelphia, PA

James T. Canaday
Engineer-Director
Alexandria Sanitation Authority
Alexandria, VA

Donnie R. Wheeler
General Manager
Hampton Roads Sanitation District
Virginia Beach, VA

REGION IV

Thomas R. Morgan
General Manager
Montgomery Water Works &
Sanitary Sewer Board
Montgomery, AL

Gordon R. Garner
Executive Director
Louisville & Jefferson County
Metropolitan Sewer District
Louisville, KY

Ray T. Orvin, Jr.
Executive Director
Western Carolina Regional Sewer Authority
Greenville, SC

REGION V

John C. Farnan
General Superintendent
Metropolitan Water Reclamation District of
Greater Chicago
Chicago, IL

William B. Schatz
General Counsel
Northeast Ohio Regional Sewer District
Cleveland, OH

Jon W. Schellpfeffer
Assistant Chief Engineer/Director of
Administration
Madison Metropolitan Sewerage District
Nine Springs Wastewater Treatment Plant
Madison, WI

REGION VI

Harold J. Gorman
Executive Director
Sewerage & Water Board of New Orleans
New Orleans, LA

David Brosman
Chief Operations Officer
El Paso Water Utilities Public Service Board
El Paso, TX

Larry Patterson
Assistant Director
Dallas Water Utilities
Dallas, TX

REGION VII

Dick Champion, Jr.
Director
Independence Water Pollution Control
Department
Independence, MO

Gurnie C. Gunter
Director
Kansas City Water Services Department
Kansas City, MO

REGION VIII

Robert W. Hite
District Manager
Metro Wastewater Reclamation District
Denver, CO

Jon G. Monson
Director, Water & Sewer Department
City of Greeley
Greeley, CO

REGION IX

Stephen T. Hayashi
General Manager/District Engineer
Union Sanitary District
Fremont, CA

Christopher Westhoff
Assistant City Attorney
City of Los Angeles Department of Public Works
Los Angeles, CA

Margaret Nellor
Assistant Department Head
Technical Services Department
Sanitation Districts of Los Angeles County
Whittier, CA

REGION X

J. Michael Read
Director
Water Environment Services of
Clackamas County
Clackamas, OR

William Gaffi
General Manager
Clean Water Services
Hillsboro, OR

William L. Pugh
Public Works Director
City of Tacoma Public Works Department
Tacoma, WA

EXECUTIVE DIRECTOR

Ken Kirk

AMSA Member Agencies

Jefferson County Commission, AL
Mobile Area Water & Sewer System, AL
Montgomery Water Works & Sanitary Sewer Board, AL
Anchorage Water & Wastewater Utility, AK
City of Mesa, AZ
City of Phoenix Water Services Dept., AZ
City of Tolleson, AZ
Pima County Wastewater Management, AZ
City of Little Rock Wastewater Utility, AR
Pine Bluff Wastewater Utility, AR
Central Contra Costa Sanitary District, CA
City of Corona Water Utilities Department, CA
City of Fontana, CA
City of Fresno Department of Public Utilities, CA
City of Los Angeles Department of Public Works, CA
City of Modesto Water Quality Control, CA
City of Oxnard, CA
City of Palo Alto, Regional Water Control Plant, CA
City of Riverside, CA
City of Sacramento, CA
City of San Diego Metropolitan Wastewater Department, CA
City of San Jose, Environmental Services Department, CA
City of Santa Barbara, CA
City of Santa Cruz, CA
City of Stockton, CA
City of Sunnyvale, CA
City of Thousand Oaks Public Works Department, CA
City of Vacaville, CA
Los Angeles County Sanitation District – Technical Services Department, CA
Delta Diablo Sanitation District, CA
East Bay Municipal Utility District, CA
Eastern Municipal Water District, CA
Encina Wastewater Authority, CA
Fairfield Suisun Sewer District, CA
Orange County Sanitation Districts Orange County, CA
Sacramento Regional County Sanitation District, CA
San Bernardino Municipal Water Department, CA
San Francisco Public Utilities Commission, CA
South Bayside System Authority, CA
South Orange County Wastewater Authority, CA
Union Sanitary District, CA
West County Wastewater District, CA
Yucaipa Valley Water District, CA
Boxelder Sanitation District, CO
City of Greeley, CO
City of Pueblo-Wastewater Department, CO
Colorado Springs Utilities, CO
Metro Wastewater Reclamation District, CO
Littleton/Englewood Wastewater Treatment Plant, CO
The Metropolitan District (Hartford County), CT
City of Wilmington Department of Public Works, DE
District of Columbia Water & Sewer Authority, DC
Broward County Environmental Services, FL
City of Boca Raton Public Utilities Department, FL
City of Altamonte Springs, FL
City of Clearwater, FL
City of Hollywood, FL
City of Jacksonville, FL
City of Orlando, FL
City of St. Petersburg, FL
City of Tallahasse Water Utilities, FL
City of Tampa Department of Sanitary Sewers, FL
Collier County Public Works Division, FL
Escambia County Utilities Authority, FL

Hillsborough County Public Utilities Department, FL

Miami-Dade Water & Sewer Department, FL

Orange County Utilities, FL

Sarasota County Environmental Services, FL

South Regional Wastewater Treatment and Disposal Board, FL

City of Atlanta, Department of Public Works, GA

Columbus Water Works, GA

Gwinnett County Department of Public Utilities, GA

Macon Water Authority, GA

Peachtree City Water & Sewerage Authority, GA

City & County of Honolulu Public Works, HI

Wastewater Reclamation Division, Wailuku, HI

City of Boise, Public Works Department, ID

City of Pocatello Water Pollution Control Department, ID

American Bottoms Regional Wastewater Treatment Facility, IL

Bloomington & Normal Water Reclamation District, IL

Danville Sanitary District, IL

Downers Grove Sanitary District, IL

Fox River Water Reclamation District, IL

Greater Peoria Sanitary District, IL

Hinsdale Sanitary District, IL

Metropolitan Water Reclamation District of Greater Chicago, IL

North Shore Sanitary District, IL

Rock River Water Reclamation District, IL

Sanitary District of Decatur, IL

Springfield Metro Sanitary District, IL

Thorn Creek Basin Sanitary District, IL

Urbana & Champaign Sanitary District, IL

Wheaton Sanitary District, IL

City of Indianapolis Deptartment of Public Works, IN

City of Valparaiso EKPCF, IN

Fort Wayne City Utilities, IN

Gary Sanitation District, IN

Sanitary District of Hammond, IN

City of Ames, IA

City of Cedar Rapids, IA

Des Moines Engineering Department, IA

City of Olathe, KS

City of Wichita, KS

Johnson County Wastewater, KS

Unified Government Wyandotte County/Kansas City, Water Pollution Control Division, KS

Lexington – Fayette Urban County Government Division of Sanitary Sewers, KY

Louisville & Jefferson County Metropolitan Sewer District, KY

Sanitation District No. 1, KY

Sewerage & Water Board of New Orleans, LA

City of Bangor, ME

Anne Arundel County Department of Public Works, MD

Howard County Department of Public Works, MD

Washington Suburban Sanitary Commission, MD

Boston Water & Sewer Commission, MA

City of Gloucester, MA

Fall River Sewer Commission, MA

Greater Lawrence Sanitary District, MA

Lowell Regional Wastewater Utility, MA

Lynn Water and Sewer Commission, MA

Massachusetts Water Resources Authority, New Bedford Wastewater Division, MA

Springfield Water & Sewer Commission, MA

South Essex Sewerage District, MA

Upper Blackstone Water Pollution Abatement District, MA

Augusta Sanitary District, ME

City of Flint, Water Pollution Control, MI

City of Grand Rapids, MI

City of Kalamazoo, MI

Detroit Water & Sewerage Department, MI

Oakland County Drain Commission, MI

Southern Clinton County Municipal Utilities Authority, MI

Van Buren Township Water & Sewer Department, MI

Wayne County Department of Environment, MI

Metropolitan Council/Enviromental Services, MN

Rochester Minnesota Water Reclamation Plant, MN

Western Lake Superior Sanitary District, MN

City of Lee's Summit Water Utilities, MO

Independence Water Pollution Control Department, MO

Kansas City Water Services Department, MO

Little Blue Valley Sewer District, MO

Metropolitan St. Louis Sewer District, MO

Sanitary Services Divison of Springfield, MO

City of Omaha Public Works Department, NE

City of Henderson, NV

City of Las Vegas Water Pollution Control Facility, NV

Clark County Sanitation District, NV

Truckee Meadows Water Reclamation Facility, NV

Nashua Wastewater Treatment Facility, NH

Atlantic County Utilities Authority, NJ

Bergen County Utilities Authority, NJ

Edgewater Municipal Utilities Authority, NJ

Ewing-Lawrence Sewerage Authority, NJ

Gloucester County Utilities Authority, NJ

Hamilton Township Wastewater Utility, NJ

Jersey City Municipal Utilities, NJ

Joint Meeting of Essex & Union Counties, NJ

Kearny Municipal Utilities Authority, NJ

Middlesex County Utilities Authority, NJ

North Bergen Municipal Utilities Authority, NJ

Ocean County Utilities Authority, NJ

Passaic Valley Sewerage Commissioners, NJ

Rahway Valley Sewerage Authority, NJ

Secaucus Municipal Utilities Authority, NJ

Somerset Raritan Valley Sewerage Authority, NJ

Stony Brook Regional Sewerage Authority, NJ

City of Albuquerque, Wastewater Utility Division Public Works Department, NM

City of Santa Fe, NM

Albany County Sewer District, NY

County of Monroe, Department of Environmental Services, NY

Great Neck Water Pollution Control, NY

Ithaca Area Wastewater Treatment, NY

New York City Department of

Environmental Protection, NY

Onondaga County Department of Drainage & Sanitation, NY

Rockland County Sewer District #1, NY

Suffolk County Department of Public Works, NY

Charlotte Mecklenberg Utilities, NC

City of Raleigh, NC

City of Salisbury, NC

Metropolitan Sewerage District of Buncombe, NC

Water and Sewer Authority of Cavarrus County, NC

Butler County Department of Environmental Services, OH

City of Akron, Public Utilities Bureau, OH

City of Canton, OH

City of Columbus, OH

City of Dayton, Department of Water, OH

City of Hamilton Department of Public Utilities, OH

City of Lebanon, OH

City of Middletown, OH

City of Troy, OH

Columbus Division of Sewerage & Drainage, OH

Metropolitan Sewer District of Greater Cincinnati, OH

Northeast Ohio Regional Sewer District, OH

Oregon Wastewater Treatment Plant, OH

Toledo Department of Public Utilities, OH

Utilities Department, City of Lima, OH

City of Oklahoma City Water & Wastewater Utilities Department, OK

City of Stillwater Utilities, OK

The City of Tulsa Public Works Department, OK

City of Albany, OR

City of Corvallis, Public Works Department, OR

City of Eugene Wastewater Division, OR

City of Gresham, OR

City of Klamath Falls, OR

City of Milwaukie, OR

City of Portland, OR

City of Salem, OR

City of Wilsonville, OR

Oak Lodge Sanitary District, OR

CLean Water Services, OR

Water Environment Services, Clackamas County, OR

Allegheny County Sanitary Authority, PA

Derry Township Municipal Authority, PA

Philadelphia Water Department, PA

The Harrisburg Authority, PA

Puerto Rico Aqueduct and Sewer Authority, PR

Narragansett Bay Commission, RI

Beaufort Jasper Water & Sewer Authority, SC

Charleston Commissioners of Public Works, SC

Greenwood Metropolitan District, SC

Mount Pleasant Waterworks, SC

Spartanburg Water System & Sanitary Sewer District, SC

Western Carolina Regional Sewer Authority, SC

City of Chattanooga, Waste Resources Division, TN

City of Johnson City, TN

City of Kingsport, TN

City of Memphis, TN

City of Oak Ridge, TN

Metro Water Services, Nashville & Davidson County, TN

Knoxville Utilities Board, Engineering & Operations, TN

Brownsville Public Utilities Board, TX

City of Amarillo, TX

City of Austin Water & Wastewater Utility, TX

City of Corpus Christi Wastewater Division, TX

City of Garland, TX

City of Houston Public Works & Engineering, Public Utilities Division, TX

City of San Antonio Water System, TX

Dallas Water Utilities, TX

El Paso Water Utilities, Public Service Board, TX

Fort Worth Water Department, TX

Gulf Coast Waste Disposal Authority, TX

Lower Colorado River Authority, TX

San Antonio Water System, TX

North Texas Municipal Water District, TX

Trinity River Authority of Texas, TX

Upper Trinity Regional Water District, TX

Weatherford Municipal Utilities, TX

Central Davis County Sewer District, UT

Central Valley Water Reclamation Facility, UT

Salt Lake City Public Utilities, UT

Snyderville Basin Water Reclamation District, UT

Burlington Public Works, VT

Alexandria Sanitation Authority, VA

Arlington Department of Environmental Services, VA

Chesterfield County Utilities, VA

City of Norfolk, VA

City of Richmond, Department of Public Utilities, VA

City of Roanoke, VA

City of Virginia Beach, VA

County of Stafford, VA

Fairfax County Integrated Sewer System, VA

Hampton Roads Sanitation District, VA

Hanover County – Department of Public Works, VA

Henrico County Wastewater Treatment Facility, VA

Hopewell Regional Wastewater Treatment Facility, VA

Pepper's Ferry Regional Wastewater Treatment Authority, VA

Prince William County Service Authority, VA

Upper Occoquan Sewage Authority, VA

City of Everett Public Works Department, WA

City of Lynnwood, WA

City of Spokane Wastewater Management, WA

City of Tacoma Public Works Department, WA

King County Department of Natural Resources, Wastewater Division, WA

Lakehaven Utility District, WA

Seattle Public Utilities, WA

Morgantown Utility Board, WV

City of Fond du Lac, WI

City of Superior – Wastewater Division, WI

Green Bay Metropolitan Sewerage District, WI

Heart of the Valley Metropolitan Sewerage District, WI

Madison Metropolitan Sewerage District, WI

Milwaukee Metropolitan Sewerage District, WI

Oak Lodge Sanitation District, WI

Racine Wastewater Utility, WI

Association of Metropolitan
Sewerage Agencies

1816 Jefferson Place, NW
Washington, DC 20036-2505
202/833-AMSA • 202/833-4657 fax
info@amsa-cleanwater.org
http://www.amsa-cleanwater.org

In association with PA Consulting Group and SCIENTECH, Inc.

PA Consulting Group

SCIENTECH®